Use These Five Backup and Recovery Best Practices to Protect Against Ransomware

Published: 8 June 2016 **ID:** G00304601

Analyst(s): Robert Rhame, Roberta J. Witty

Ransomware is on the rise, and its perpetrators are effectively evading countermeasures. I&O and business continuity management leaders should plan for the inevitable limited or widespread ransomware incident.

Key Challenges

- Incumbent antivirus prevention techniques cannot be relied upon to detect and stop all ransomware.
- A single infected client can encrypt all file shares they have access to, potentially including cloud storage locations.
- Once files are encrypted, organizations have two choices: restore from a backup or pay up.
- Ransomware is generating huge revenue for criminals and it should be expected that these attacks will intensify in volume and sophistication.

Recommendations

- Ensure that your organization has a single dedicated crisis management team.
- Implement an enterprise endpoint backup product to protect user data on laptops and workstations.
- Build a list of storage locations that users can connect to that are inherently vulnerable, such as file shares.
- Evaluate the potential business impact of data being encrypted due to a ransomware attack, and adjust recovery point objectives (RPOs) to more frequently back up these computer systems.
- Align with the information security, IT disaster recovery and network teams to develop a unified incident response that focuses on resiliency, not only prevention.

Introduction

Users are only a click away from a drive-by download of malware from a compromised web page, or a postlunch launch of a trojan attachment from a ransomware spam campaign. The rapid-release nature of the malware underground means that antivirus vendors are playing a game of catch-up. The ransomware authors only have to be successful in bypassing defenses once, and they change their tactics constantly in order to do so. Organizations must assume accidents will happen, and that their data will be held for ransom.

Ransomware has emerged in the past few years. It is a form of malware where files are encrypted and then a bitcoin ransom is demanded in return for the decryption key. There are two types of attack mechanisms for ransomware:

- In the more common scenario, an end user is duped into clicking an attachment or visits the wrong web page resulting in his/her laptop or workstation and all connected file shares being encrypted.
- The less common scenario to date is a targeted approach where hackers get inside the organization and then use encryption of data as a tool to force payment.

So far, most ransomware authors prefer to cash out, so they immediately and prominently inform the victim that files have been encrypted. Some might use threats or scare tactics — such as setting a deadline after which the data will be permanently lost — encouraging a sense of urgency and keeping the victim off balance. Some ransomware may even use tactics to try to avoid detection long enough that backup retention expires before demanding a ransom.

Your first impulse might be to increase backup retention, but, on reflection, it is hard to imagine having to restore a backup that is older than 90 or 120 days. Instead of making these kinds of blanket changes, it is important for organizations to first understand what type of data storage is typically affected by a ransomware attack.

Typical Data Storage Affected

In most cases, the initial ransomware attack occurs on a user's laptop or workstation. Therefore, locally stored data in files and folders, file shares, cloud storage via gateways, as well as any mapped network drives, is inherently vulnerable.

Data Affected Because of Replication

Enterprise file synchronization and sharing (EFSS) in and of itself is not vulnerable since an agent handles the communication with the on-site or in-the-cloud synch and share server. In this case, there is no mount point for the ransomware to traverse; however, the replication mechanism will replicate changes made locally as part of the functionality, thereby replicating the encrypted files (and, possibly in the future, also malware) to the shared directories. EFSS typically has versioning capabilities, but not bulk restore. A laptop restored using endpoint backup will replicate the last good versions as a new file change, but there may be scenarios where cleaning up the versions to a known clean state will be desired.

Not Vulnerable Today

SharePoint or any web application where end users' access is through an authenticated web browser session is not vulnerable to a ransomware attack yet. As the countermeasures evolve, ransomware attackers might begin including a remote access trojan (RAT) in the malware in order to manually remote control the infected host and overcome limitations of an automated attack. A similar tactic was used with banking trojans when countermeasures began to reduce effectiveness of the automated approach. This is a very manual process for the attackers, requires a connection to the infected host and does not scale.

Follow the five backup and recovery best practices documented in this research to ensure that you are as protected as possible from ransomware attacks.

Analysis

Step 1: Form a Single Crisis Management Team

An effective response to the ransomware threat must be a holistic and multilevel one — reducing the likelihood of a successful attack to the bare minimum, while simultaneously ensuring the ability to recover from an unprevented attack. IT operations and IT disaster recovery (IT DR) must work with their counterparts in information security to develop an integrated response and recovery approach, including a framework for responding to all new threats and a continuously updated risk assessment of the IT infrastructure vulnerable to a ransomware attack. To deal with the changing threat landscape that touches the entire organization, the creation of a single crisis management team comprising IT operations, IT DR and infosec is no longer an optional action (see "Prepare for and Respond to a Business Disruption After an Aggressive Cyberattack").

Step 2: Implement Endpoint Backup

Without a backup, years of locally stored files and folders on a laptop/workstation would be lost; that is, unless the organization wants to pay to release them, fueling the ransomware economy. Even without ransomware, complications and costs from potential disclosure resulting from loss, theft and hard drive crashes can quickly help build a compelling case for deploying laptop and workstation backup. Therefore, implementing endpoint backup solutions will ensure you have a safe copy of your data that can be restored once faced with the threat.

Depending on the endpoint backup product's capabilities, backup schedules based on your organization's RPOs can be configured to run at intervals of several times an hour, several times a day, or during idle laptop/workstation cycles. The decision must be made as to what time frame is an acceptable loss for the organization based on the recovery requirements for that user group.

Endpoint backup can provide two key functions:

- **Laptop or workstation restore —** After the ransomware infection has been remediated, all files up to the last backup can be restored.

- **EFSS upstream replication —** Once the restore is completed, the administrator can reconnect the user to his/her synch and share application. The restored files will synchronize from the local EFSS folder to the user's directories, thereby replacing the encrypted files.

Endpoint backup solutions can be configured to back up mapped drives (such as home folders or file shares) to accelerate returning a single employee back to production, but they do not replace a centralized solution in case of an overall storage failure or wider infection.

Justification for the investment in endpoint backup can be calculated using the following metrics:

- Productivity loss per employee for all involved
- Salaries of each employee involved
- Time involved to recreate content
- The number of estimated ransomware incidents, accidental deletions, hard drive crashes or laptop losses/thefts

Refer to "How to Address Three Key Challenges When Considering Endpoint Backup" to learn more about this cost calculation algorithm.

Step 3: Identify Network Storage Locations and Servers Vulnerable to Ransomware Encryption

Enumerate Obviously Vulnerable Storage Locations

The most important task is to revisit RPOs for potentially vulnerable storage locations. Following the laptop or workstation infection, the ransomware traverses all mount points configured in Windows Explorer in an attempt to encrypt everything it finds. A first assessment can be done by talking to the Active Directory and/or PC deployment group to find out what the standard Group Policy Mapped Drives are for each new laptop or workstation image. This task provides an inventory of servers for further investigation. These file share servers should then be audited for overly permissive inherited permissions that could allow unnecessarily broad file and folder traversal (and encryption of everything where "modify" or "full" permissions are set). Work with the Directory Services team to tighten permissions where possible, but realize not everything can be fully restricted without full knowledge of who needs access to what directories and their criticality to business operations. Then, move on to an evaluation of this server's backup policy.

Don't Forget the Not-So-Obvious Vulnerable Storage Locations

A single mapped drive could cause unexpected servers to be affected. It is common for database and application administrators (and consultants) to map drives to work with full system privileges at the file system level in order to perform installs, maintenance, upgrades or troubleshooting of the software/applications that they are working on. If an administrator has a drive mapped "persistently" (the box "reconnect at logon" is checked) and his/her workstation gets infected, then data on any mapped drive will also be encrypted. If cross-zone drive mapping is allowed, you must communicate to all privileged users that they should not use persistent mapping, and then

disconnect these drives rather than leaving them open for their entire user session. We advise working with the IT network team to get a list of potential servers reachable from the user zone via TCP port 445 (used for SMB over TCP), but it does require that basic network segmentation is in place.

Step 4: Develop Appropriate RPOs and Backup Cadences for Network Storage and Servers

The next step is to re-examine your organization's RPOs for appropriateness to the business function. It is likely that file shares are only backed up nightly; therefore, if they are actively used as an ad hoc collaboration system, then a loss could hurt the organization worse than expected because of the greater potential for losing new and modified data. There are two steps to this task:

- First, determine how much data loss the organization will accept. While never a comfortable exercise, the reality is that the greater your loss avoidance risk position, the more likely a solution will require more resources (for example, budget and administration).
- Second, set the RPOs for each server deemed to be at greater risk to ransomware, and according to organizational requirements based on a data loss time frame that is acceptable to the organization.

The primary goal is to leverage newer backup methodologies to achieve more frequent recovery points. This may mean acquiring new technology, or simply fully deploying capabilities of the existing storage and backup solutions already in place. The goal here is backing up more often.

Identify the fast file scan, changed block tracking and snapshot capabilities that are available for storage arrays with the enterprise backup application, and if "incremental forever" or "virtual synthetic full" backup options are possible. If available, leverage fast-scan capabilities to back up only changed files or changed block tracking for storage arrays and/or virtual machines (VMs) in order to schedule more frequent backups. This will allow for more frequent backups (including during the day) while requiring fewer resources, and, thus, will offer greater protection.

It is advisable to implement less predictable backup times with at least one RPO during the day, when new infections are most likely to occur. Rudimentary time-based encryption/decryption cycles have been observed in some ransomware attacks, most likely to masquerade the ransomware's presence for as long as possible; thereby increasing the time frame of data loss and potentially reaching a threshold when organizations decide to pay up rather than restore from old backups.

For selected workloads, tactically implement new technologies that can step backward to recovery points, such as continuous data protection (CDP), hyperconverged integrated systems (HCIS), hypervisor-based replication products, or DR replication that includes change journaling.

There have been a few reports that perpetrators are encrypting backed-up data before triggering the ransomware attack to encrypt production data. The result of this added step in the attack process could mean that the most current backups won't be of value, and restore will have to be done from older or offline versions. However, Gartner believes that this added step of encrypting or deleting backed-up data is a long way off in reality (refer to Note 1 for our explanation).

As an overall defense, Gartner's best practice for backup is to have at least two copies of your backed-up data geographically dispersed to mitigate against a broad range of natural and man-made disasters. Ideally, at least one copy of the backed-up data is offline and off-site to reduce the impact of accidental or malicious destruction. Some organizations elect to have backed-up data on two or more different kinds of technology or media to reduce infrastructure or vendor dependencies.

Step 5: Create Reporting Notifications for Change Volume Anomalies

For future ransomware attacks, there might not be a ransom demand immediately; therefore, it is imperative that the activity be noticed quickly. Combined with running select backups during the day, reporting on storage anomalies can help identify that an attack has occurred or is actively underway. Implementing such reports includes three tasks:

- Create a report in your enterprise backup application that will trigger an alert when a high number of changes occurring on servers results in a sudden and marked increase in storage.
- Create reports based on capacity thresholds for devices that use deduplication, such as backup target appliances and HCIS, since unexpected encryption will result in 100% change rate and a large increase in storage consumption.
- Examine the reporting capabilities available in your endpoint backup application and EFSS, and implement a storage anomaly report.

Share this extra dimension of reporting with the infosec group, as it complements the countermeasures and detection systems it has in place.

Additional research contribution and review by Pushan Rinnen and Dave Russell.

Acronym Key and Glossary Terms

File Share	A folder shared for a single user or a group of users with permissions.
Mapped Drive	A drive that is mapped through the network to a file storage location. These drives should be configured to reconnect at logon. Another common practice is deployment of Home Directories as part of an Active Directory Group Policy.

Gartner Recommended Reading

Some documents may not be available as part of your current Gartner subscription.

"Critical Capabilities for Enterprise Endpoint Backup"

"How to Address Three Key Challenges When Considering Endpoint Backup"

"Prepare for and Respond to a Business Disruption After an Aggressive Cyberattack"

"Predicts 2016: Business Continuity Management and IT Service Continuity Management"

"Toolkit: Security Incident Response Roundtable Scenario for Malware"

"Designing an Adaptive Security Architecture for Protection From Advanced Attacks"

"Magic Quadrant for Endpoint Protection Platforms"

Evidence

Since 2005, the Internet Crime Complaint Center (IC3) has had 7,694 ransomware complaints totaling $57,602,032.72. While the ransom fees are typically between $200 and $10,000, victims include in their complaints additional costs they incurred due to the ransomware incident. These additional costs include network mitigation, network countermeasures, loss of productivity, legal fees, information technology services, and/or the purchase of credit monitoring services for employees or customers. Additionally, victims sometimes will put a price on the data that was encrypted due to its perceived importance, making it difficult to determine the actual cost to victims associated with a ransomware incident.

Note 1 Encrypting Backups as Part of a Ransomware Attack

There have been a few reports that perpetrators are encrypting backed-up data before initiating the ransomware attack on production data. The result of this added dimension in the attack process could mean that the most current backups won't be of value, and restore will have to be done from older versions. While it is prudent to assume the criminal community is actively researching how to accomplish this in an automated manner, Gartner believes that the sophistication required to automatically target and encrypt backed-up data is a long way off in reality.

The reason for this position follows: The backup and recovery market comprises hundreds of vendors. In order to "attack" backup, adversaries would have to have a good bit of knowledge about how the backup applications work in a production environment. Disabling or tampering with an agent for an unknown system is not easy to automate, and many backups (particularly for VMs hosted in a hypervisor) occur agentlessly. That leaves a media server or proxy as the next step up the chain, which, if successfully attacked, would terminate all running backups, resulting in error messages and notifications being sent to many IT operations monitoring points. Getting access to the backup server would require knowing the server's name, and then knowing how to cause a failure of some sort. Frequently, the actual backup data is stored on target appliances and also tape, so there is another step of abstraction and another dimension of complexity, preparation and testing for the attackers. All of this combined would mean that an automated attack on backup infrastructure is unlikely. A full breach followed by systematic elevation of privilege would be required.

Follow the recommendations in this research to educate backup system administrators and operators to avoid using persistently mapped drives to the backup servers.

More on This Topic

This is part of an in-depth collection of research. See the collection:

- Special Report: Cybersecurity at the Speed of Digital Business

GARTNER HEADQUARTERS

Corporate Headquarters
56 Top Gallant Road
Stamford, CT 06902-7700
USA
+1 203 964 0096

Regional Headquarters
AUSTRALIA
BRAZIL
JAPAN
UNITED KINGDOM

For a complete list of worldwide locations,
visit http://www.gartner.com/technology/about.jsp